What is claimed is:

1. A data transfer apparatus for secure transfer, from a digital data source to a digital data receiver, of a plurality of data blocks, the apparatus comprising:

(a) an encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks and a block synchronization index indicating a correspondence between said encryption key and said single data block;

(b) an encryption engine that, for each said single data block, produces an encrypted data block using said encryption key from said encryption key genefator;

(c) a data transmission channel for delivering said encrypted data block from said encryption engine to the digital data receiver;

(d) a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver; and

(e) a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver.

2. The apparatus of claim 1 wherein said digital data receiver includes a decryption engine which is responsive to said encryption key and said encryption engine and decryption engine are provided with symmetric encryption.

3. The apparatus of claim 1 wherein the size of said single data block is further conditioned by an offset value.

4. The apparatus of claim 1 wherein said single data block comprises video data.

5. The apparatus of claim 1 wherein said data transmission channel is a wireless transmission network.

6. The apparatus of claim 1 wherein said data transmission channel utilizes dedicated phone service.

7. The apparatus of claim 1 wherein said data transmission channel utilizes a portable storage medium.

8. The apparatus of claim 1 wherein said data transmission channel utilizes a computer data network.

9. The apparatus of claim 1 wherein said data transmission channel utilizes a local area network.

10. The apparatus of claim 1 wherein said data transmission channel utilizes a wide area network.

11. The apparatus of claim 1 wherein said block synchronization transmission channel utilizes a smart card.

12. The apparatus of claim 1 wherein said block synchronization data is encrypted.

13. The apparatus of claim 1 wherein said block synchronization transmission channel utilizes a portable storage medium.

14. The apparatus of claim 1 wherein said key synchronization transmission channel utilizes a smart card.

15. The apparatus of claim 1 wherein said key synchronization data is encrypted.

16. The apparatus of claim 1 wherein said key synchronization transmission channel utilizes a portable storage medium.

17. The apparatus of claim 1 wherein said single data block is compressed.

18. The apparatus of claim 1 wherein said block synchronization index is computed using a pseudo-random number generator.

19. The apparatus of claim 18 wherein said pseudo-random number generator is a linear feedback shift register.

20. A method for secure transfer of a data stream from a digital data source to a digital data receiver, the method comprising:

(a) partitioning the data stream into a plurality of successive data blocks, wherein the size of each successive data block is variable, based on an average size and based on a randomly generated offset;

(b) generating, for each successive data block, an encryption key;

(c) encrypting each said successive data block using said encryption key to provide an encrypted data block; and

(d) generating a synchronization index associating said encrypted data block with said encryption key.

21. The method of claim 20 wherein the step of providing said encrypted data block comprises the step of recording said encrypted data block onto a recording medium.

22. The method of claim 21 wherein said recording medium uses a magnetic storage technology.

23. The method of claim 21 wherein said recording medium uses an optical storage technology.

24. The method of claim 20 wherein the step of providing said encrypted data block comprises the step of transmitting said encrypted data block to the digital data receiver.

25. The method of claim 20 further comprising the step of encrypting said encryption key.

26. The method of claim 20 further comprising the step of transmitting said encrypted data blocks to said receiver site in non-sequential order.

27. The method of claim 20 wherein said data stream comprises digital motion image data.

28. A method for secure transfer of a digital motion image data stream from a digital data source to a digital data receiver, the method comprising:

(a) partitioning the digital motion image data stream into a plurality of digital motion image data blocks;

(b) generating a plurality of encryption keys;

(c) generating an encrypted digital motion image data stream by a repetition of the following steps (1) and (2) for each of said plurality of digital motion image data blocks:

(1) encrypting each said digital motion image data block using a distinct encryption key to create an encrypted video data block;

(2) storing said encrypted data block as part of said encrypted digital motion image data stream;

(d) generating a synchronization index that associates each said digital motion image data block with each said distinct encryption key;

(e) providing said encrypted digital motion image data stream to the digital data receiver;

(f) providing said synchronization index to the digital data receiver.

29. The method of claim 28 wherein the step of partitioning the digital motion image data stream into a plurality of digital motion image data blocks further comprises:

(a) generating an offset value used to establish a starting frame for each said digital motion image data block.

30. The method of claim 28 wherein the step of partitioning the digital motion image data stream into a plurality of data blocks uses a digital motion image frame as a base unit.

31. The method of claim 28 wherein the step of generating a synchronization index further comprises encrypting said synchronization index.

32. The method of claim 28 wherein the step of providing said encrypted digital motion image data stream to the digital data receiver comprises the step of transmitting said encrypted digital motion image data stream.

33. The method of claim 28 wherein the step of providing said encrypted digital motion image data stream to the digital data receiver comprises the step of recording said encrypted digital motion image data stream onto a storage medium.

34. The method of claim 28 wherein the step of providing said synchronization index to the digital data receiver comprises the step of transmitting said synchronization index.

35. The method of claim 28 wherein the step of providing said synchronization index to the digital data receiver comprises the step of recording said synchronization index onto a storage medium.

36. A method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks, the method comprising:

(a) providing said plurality of encryption keys separately from said encrypted data blocks; and

(b) providing an identifier that correlates a mapping algorithm to said plurality of encryption keys.

37. The method of claim 36 wherein said plurality of encryption keys are interleaved in a non-sequential order.

38. The method of claim 36 further comprising the step of padding said plurality of encryption keys using dummy bits.

39. The method of claim 36 and wherein the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part.

40. The method of claim 39 wherein each block is a digital motion image data frame component of a motion picture.

41. The method of claim 39 wherein each block is a digital motion image data frame of a motion picture.

42. The method of claim 39 wherein decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen.

43. The method of claim 39 wherein the digital motion image data blocks comprise data of a motion picture in compressed form and the entire motion picture is encrypted.

44. The method of claim 39 wherein the digital motion image data blocks are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra- coded and P and B frames are encrypted.

45. The method of claim 39 wherein a digital motion image data frame comprises plural color components and only data of one of the color components is encrypted.

46. The method of claim 45 wherein the color component that is encrypted is represented by a bit depth greater than one and only one or more bit planes but less than all bit planes of the color component data is encrypted.

47. A method of decrypting encrypted digital motion image data blocks of a motion picture comprising:

providing a digital motion image data frame or digital motion image data frame component identification; and

generating a corresponding key from a plurality of encryption keys for use in decrypting a digital motion image data block of which the digital motion image data frame or digital motion image data frame component forms a part.

48. The method of claim 47 wherein each block is a digital motion image data frame component of the motion picture.

49. The method of claim 47 wherein each block is a digital motion image data frame of the motion picture.

50. The method of claim 47 wherein the decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen.

51. The method of claim 47 wherein the digital motion image data blocks comprise data of the motion picture in compressed form and the entire motion picture is encrypted.

52. The method of claim 47 wherein the digital motion image data blocks are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra- coded and P and B frames are encrypted.

53. The method of claim 47 wherein a digital motion image data frame comprises plural color components and only data of one of the color components is encrypted.

54. The method of claim 53 wherein the data of the color component that is encrypted is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of the color component data is encrypted.

55. The method of claim 47 wherein a digital motion image data frame comprises plural color components and the data of the color components are encrypted.

56. The method of claim 55 wherein each color component is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of each color component data is encrypted.

57. The method of claim 47 wherein block boundaries have variable offset relative to correspondence of location in a frame.

58. The method of claim 47 wherein indices providing correspondence information relative to encryption keys are provided in a channel separate from a channel providing ciphertext of the encrypted data blocks.

59. The method of claim 47 wherein a data block represents plural frames of the motion picture.

60. The method of claim 59 wherein the data blocks are of different sizes.

61. The method of claim 60 wherein block boundaries have variable offset relative to correspondence of relative location in a frame.